UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/706,503	11/02/2000	David J. Wetherall	0016.0005US1	8089

29127 7590 04/01/2009

HOUSTON ELISEEVA
4 MILITIA DRIVE, SUITE 4
LEXINGTON, MA 02421

EXAMINER	
BIAGINI, CHRISTOPHER D	

ART UNIT	PAPER NUMBER
2442	

MAIL DATE	DELIVERY MODE
04/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/706,503	WETHERALL ET AL.	
	Examiner	Art Unit	
	Christopher Biagini	2442	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,5-14,16,18-27,29,31-39,42-48 and 51-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,5-14,16,18-27,29,31-39,42-47 and 51-57* is/are rejected.

7)☒ Claim(s) *48 and 57* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Remarks

In view of the appeal brief filed on December 12, 2008, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below.

Response to Arguments

Applicant's arguments regarding the rejections of claims 1, 14, 27, and 58 under 35 USC 103(a) have been fully considered but are not persuasive.

Applicant argues that each of the independent claims "requires the detection of a DoS attack at a routing device that is at the boundary between a network domain and a public internetworking fabric" and that "the prior art references teach the detection of the DoS attack at or near the target of the attack" (as opposed to detection near the source of the attack). The Examiner respectfully disagrees. Malan explicitly indicates that the StormDetector system (which detects the DoS attack) may be "employed at an attacker's originating network." Malan also discloses that StormDetector may be "used in both source and transit networks." See discussion of "StormDetector" on p. 12 (as scanned) of application No. 60/231,480, to which Malan claims priority. Indeed, Malan even recognizes the benefits of detecting the attack at the source, indicating that the system "allows network providers and enterprise managers to identify gross bandwidth anomalies": see p. 11 of application No. 60/231,480.

Incidentally, Poletto also teaches detection at the source of the attack. For example, Poletto teaches that gateways 26 conduct monitoring to detect DoS attacks (see [0044]), and that attackers can be behind a gateway 26 (see [0042]).

The Examiner notes that in an effort to advance prosecution, the citations to Malan and Poletto used in the rejections below have been amended for clarity. The Examiner also wishes to note that Appellant admits that the method used to detect DoS attacks (by way of differential characteristics) is not new in itself (see page 9 of Appeal Brief filed December 12, 2008).

Applicant's arguments regarding the rejections of claims 6, 19, and 32 have been fully considered and are persuasive. Accordingly, the rejections are withdrawn. However, upon further consideration, a new ground(s) of rejection is made.

Applicant's arguments regarding the rejections of claims 44 and 53 have been fully considered and are persuasive. Accordingly, the rejections are withdrawn. However, upon further consideration, a new ground(s) of rejection is made.

Applicant's arguments regarding the rejections of claims 46, 55, and 58 have been fully considered and are persuasive. Accordingly, the rejections are withdrawn. However, upon further consideration, a new ground(s) of rejection is made.

Applicant's arguments regarding the rejections of claims 46, 55, and 58 have been fully considered and are persuasive. Accordingly, the rejections are withdrawn. However, upon further consideration, a new ground(s) of rejection is made.

Applicant's arguments regarding the rejections of claims 48 and 57 have been fully considered and are persuasive. Accordingly, the rejections are withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3, 5, 10-16, 18, 27, 29, 31, 36-39, 42, 43, 47, 51, 52, 56, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (US Pub. No. 2002/0032871, hereinafter "Malan") in view of Poletto et al. (US Pub. No. 2002/0032880, hereinafter "Poletto").

Note that Malan claims priority to and incorporates by reference three provisional applications: Nos. 60/231,479, 60/231,480, and 60/231,481, all filed on September 8, 2000. Except where noted below, all page and line numbers cited in connection with Malan refer to those in application No. 60/231,680. Since the numbering of the pages is inconsistent throughout the application, the numbers will refer to the pages as they were scanned into the PTO records (i.e., with page 1 being the cover sheet).

Similarly, Poletto claims priority to and incorporates by reference provisional application No. 60/230,759, filed September 7, 2000. Except where noted below, all page and line numbers cited in connection with Poletto refer to those in application No. 60/230,759. Since the numbering of the pages is consistent throughout the application, the numbers will refer to the pages as they are labeled (i.e., with page 1 corresponding to the third scanned sheet in the application).

Regarding claim 1, Malan shows:

- a first network domain which is a local area network (for example, an enterprise network: see first paragraph under "StormDetector" on p. 12);
- a first routing device (comprising an attacker's router) at a boundary between the first network domain and public internetworking fabric (comprising an ISP network: see Fig. 4 and the paragraph spanning pp. 14-15) to route network traffic between the first

network domain and the public internetworking fabric (implicitly disclosed as the typical functionality of a first-hop router: see last paragraph on p. 12);

- a monitor/regulator (comprising the StormDetector analysis engine), either integrally disposed in said first routing device or coupled to the first routing device (see second paragraph under "StormDetector" on p. 12 and Figs. 2 and 4) to monitor the network traffic routed by said first routing device by analyzing flow records (comprising "flow statistics": see second and third paragraphs under "StormDetector" on p. 12 and note that StormDetector can be used in "source and transit networks" and "an attacker's originating network"), describing traffic conversation as indicated by a combination of source and destination addresses (comprising "flow statistics" as described above, further explained as being indicated by a combination of source and destination addresses in the paragraph spanning pp. 3-4), received from the routing device (note that the analysis engine receives flow statistics from all the routers in the attack path, including the attacker's router: see "StormProfiler" on p. 11), the monitor/regulator determining if the first network domain is sourcing undesirable network traffic (comprising determining that the attack originates in the enterprise network: see paragraph spanning pp. 14-15), comprising a denial of service attack in which the undesirable network traffic is launched against a target network device (for example, a target web hosting server: see "StormDetector" on p. 12 and "StormBreaker" on p. 14) in order to undermine the operation of that target network device by overwhelming the target network device with network traffic (typical of denial of service attacks, and further explained at the first paragraph on p. 3), out of the first

network domain (note that the attacker must send the traffic out of the enterprise network in order for it to reach the web host).

Malan shows wherein said monitor/regulator makes said determination based on identifying malicious traffic at the routing device using network profiling (see "StormDetector" on p. 12, and note that StormDetector "instantly identify[ies] malicious traffic" and can be "employed at an attacker's originating network"), but does not explicitly show wherein said monitor/regulator makes said determination based on differential characteristics of network traffic routed out of said first network domain relative to network traffic routed into said first network domain and aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

Poletto shows identifying malicious traffic at a routing device (comprising a gateway) based on differential characteristics of network traffic routed out of a domain relative to network traffic routed into the domain (comprising a ratio of request packets to acknowledgement packets), and aggregating said differential characteristics (comprising maintaining an analysis of the ratio over time) based on differential characteristics between request packets routed out of said network domain (comprising client request packets which are routed out of an attacker's domain), and response packets routed into the network domain (comprising server acknowledgement packets which are routed into the attacker's domain: see pages 15-16).

Because both Malan and Poletto teach methods for identifying malicious traffic at a routing device, it would have been obvious to one of ordinary skill in the art to substitute one

method for the other in order to achieve the predictable result of determining that the network domain is sourcing undesirable traffic.

Regarding claim 3, the combination further shows wherein said monitor/regulator infers said differential characteristics based on aggregated statistics of said network traffic routed out of said network domain, and aggregated statistics of said network traffic routed into the network domain (comprising maintaining an analysis of the ratio over time, which necessarily involves maintaining information about the number of packets routed into and out of the domain). Note that in the combination described above, the ratio monitoring process of Poletto is executing on the routers of Malan, including the attacker's router. Thus, a request packet from the attacker would be routed out of the attacker's network domain (such as the enterprise network), and response packets would be routed into the attacker's network domain.

Regarding claim 5, the combination further shows wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of said first domain, further stops said undesirable network traffic from being sourced out of said first domain (see Malan, paragraph spanning pp. 14-15).

Regarding claim 10, the combination further shows wherein

- said network further comprises a second network domain (ISP-B) including a second routing device (comprising a router in ISP-B) for routing network traffic out of and into the second network domain (see Fig. 2 on p. 13 of Malan);

- said monitor/regulator further monitors the network traffic routed by said second routing device (note that the system of Malan monitors traffic statistics sent from ISP routers: see second paragraph on p. 11 and Fig. 2 of Malan), and determines if at least a selected one of the first and second network domains is sourcing undesirable network traffic out of the selected one of the first and second network domains based on network traffic characteristics observed of network traffic routed through said first and second routing devices (comprising determining that the first network is the location of the attacker: see "StormDetector" on p. 12 of Malan).

Regarding claim 11, the combination further shows wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device (note that the analysis engine collects statistics from all routers in the attack path in order to track attacks to their source: see “StormTracker” on p. 13 of Malan).

Regarding claim 12, the combination further shows wherein said monitor/regulator determines if undesirable network traffics are being routed out of said second network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device (note that the analysis engine collects statistics from all routers in the attack path in order to track attacks to their

source, and further note that the system would detect the source of the attack regardless of which domain it originated in: see "StormTracker" on p. 13 of Malan).

Regarding claim 13, the combination further shows wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of at least a selected one of said first and second network domains, further stops said undesirable network traffic from being sourced out of said first and second network domains (see paragraph spanning pp. 14-15, and note that the system would stop traffic at the source of the attack regardless of which domain it originated in).

Regarding claim 42, the combination further shows wherein said monitor/regulator generates statistics concerning destination addresses and determines whether the first network domain is sourcing undesirable network traffic based on said statistics (see discussion of "flow-based statistics" in paragraph spanning pp. 3-4 of Malan).

Regarding claim 43, the combination further shows wherein said monitor/regulator generates statistics concerning lengths of packets and determines whether the first network domain is sourcing undesirable network traffic based on said statistics (see discussion of "single packet statistics" in paragraph spanning pp. 3-4 of Malan).

Regarding claim 47, the combination further shows wherein said monitor/regulator instructs a routing device to slow the undesirable network traffic (comprising slowing the attack traffic to zero: see paragraph spanning pp. 14-15 of Malan).

Claims 14, 16, 18, 27, 29, 31, 36-39, 51, 52, and 56 correspond to claims 1, 3, 5, 10-13, 42, 43, 47 and are rejected for the same reasons as given above.

Claim 58 is an apparatus claim which corresponds to claim 1 as addressed above. However, the claim includes the additional limitations of (a) the monitor/regulator generating statistics concerning destination addresses to determine whether the network domain is sourcing the undesirable network traffic, and (b) wherein said monitor/regulator instructs the routing device to lower a priority of the undesirable network traffic and/or slow the undesirable network traffic. It is noted that Malan teaches these additional features. Malan teaches the monitor/regulator generating statistics concerning destination addresses to determine whether the network domain is sourcing the undesirable network traffic (see discussion of "flow-based statistics" in paragraph spanning pp. 3-4), and further teaches wherein said monitor/regulator instructs the routing device to slow the undesirable network traffic (comprising slowing the attack traffic to zero: see paragraph spanning pp. 14-15).

Claims 6-9, 19-26, and 32-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan (US Pub. No. 2002/0032871) in view of Poletto (US Pub. No. 2002/0032880), and further in view of Li (US Patent No. 5,473,599).

Regarding claim 6, the combination does not show wherein said first network domain further comprises a second routing device for routing network traffic out of and into the first network domain; and said monitor/regulator further monitors the network traffic routed by said second routing device, and determines if the first network domain is sourcing undesirable network traffic out of the first network domain based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

Li shows a network domain comprising a second routing device for routing network traffic out of and into the network domain (see col. 7, lines 30-45). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Malan with the second routing device taught by Li in order to reduce the burden on the first routing device.

Note that such a combination would result in said monitor/regulator further monitoring the network traffic routed by said second routing device, and determining if the first network domain is sourcing undesirable network traffic out of the first network domain based on network traffic characteristics observed of network traffic routed through said first and second routing devices, since Malan teaches that all the routers in a network's routing infrastructure are used for collecting data: see first paragraph under "StormProfiler" on p. 11).

Regarding claim 7, the combination further shows wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network

traffic routed through said second as well as said first routing device (note that all the routers in a network's routing infrastructure are used for collecting data: see first paragraph under "StormProfiler" on p. 11).

Regarding claim 8, the combination further shows wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device (note that the analysis engine collects statistics from all routers in the attack path in order to track attacks to their source: see "StormTracker" on p. 13 of Malan).

Regarding claim 9, the combination further shows wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of said first network domain, further stops said undesirable network traffic from being sourced out of said first network domain (note that the analysis engine collects statistics from all routers in the attack path in order to track attacks to their source, and further note that the system would detect the source of the attack regardless of where it originated: see "StormTracker" on p. 13 of Malan).

Claims 19-26 correspond to claims 6-13 and are rejected for the same reasons as given above.

Claims 32-35 correspond to claims 6-9 and are rejected for the same reasons as given above.

Claims 44 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan (US Pub. No. 2002/0032871) in view of Poletto (US Pub. No. 2002/0032880), and further in view of Carr (US Patent No. 5,293,379).

Regarding claim 44, the combination further shows wherein said monitor/regulator generates statistics concerning distributions of various fields in TCP/IP packet headers (see discussion of "single-packet statistics" in paragraph spanning pp. 3-4 of Malan) and determines whether the first network domain is sourcing undesirable network traffic based on said statistics, but does not show that the statistics are generated using time to live values.

Carr shows that TCP/IP packet headers include time to live values (see Fig. 4 and col. 5, lines 27-36). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the TTL field taught by Carr along with the statistics generation taught by Malan in order to provide an additional basis for determining that traffic is malicious.

Claim 53 corresponds to claim 44 and is rejected for the same reason as given above.

Claims 45 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan (US Pub. No. 2002/0032871) in view of Poletto (US Pub. No. 2002/0032880), and further in view of Galloway (US Patent No. 5,430,709).

Regarding claim 45, the combination further shows wherein said monitor/regulator tracks differences between outbound transmission control protocol (TCP) synchronize (SYN) and inbound response packets (ACKs) and determines whether the first network domain is sourcing undesirable network traffic based on said differences (see Poletto, pp. 16-17).

The combination does not show tracking differences between finish (FIN) packets and inbound response packets.

Galloway shows that finish (FIN) packets should elicit ACK packets in response (see Fig. 3). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Malan to track FIN packets in order to provide an additional basis for determining that traffic is malicious.

Claim 54 corresponds to claim 45 and is rejected for the same reason as given above.

Claims 46 and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan (US Pub. No. 2002/0032871) in view of Poletto (US Pub. No. 2002/0032880), and further in view of Katoh et al. (US Patent No. 5,949,757, hereinafter "Katoh").

Regarding claim 46, the combination does not show wherein monitor/regulator instructs a routing device to lower a priority of the undesirable network traffic.

Katoh shows lowering a priority of undesirable network traffic (see col. 4, lines 10-13). It would have been obvious to one of ordinary skill in the art at the time of the invention to further

modify the system of Malan to lower the priority of undesirable traffic as taught by Katoh in order to achieve the predictable result of easing congestion caused by the attack without running the risk of blocking innocent traffic entirely.

Claim 55 corresponds to claim 46 and is rejected for the same reason as given above.

Allowable Subject Matter

Claims 48 and 57 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter: the art of record does not teach or suggest a combination as claimed, wherein a monitor/regulator, upon determining undesirable network traffics are being sourced out of at least a selected one of said first and second network domains, lower a threshold for concluding that undesirable network traffic are being sourced out of an other one of said first and second network domains.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER D. BIAGINI whose telephone number is (571)272-9743. The examiner can normally be reached on weekdays from 8:30 AM to 5:00 PM..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew Caldwell/
Supervisory Patent Examiner, Art Unit 2442

Christopher Biagini
(571) 272-9743